Supplementary Reference: 552
File Name: 552sad_040500
Last Revised: 04/05/2000

CLASSIFIED PROCESSING COMPLIANCE REVIEW

This questionnaire was developed by M/IRM/IPA (security) in coordination with the Office of Security (SEC) to evaluate implementation of and compliance with the Federal and USAID automated information systems security policies, procedures and regulations governing electronic processing and storage of classified national security information.

The site ISSO, in conjunction with the System Manager/IT Specialist and appropriate security personnel, shall use this questionnaire as a guideline for conducting an annual review of the security posture of each system authorized to process classified national security information. The completed questionnaire shall be retained, along with a plan for corrective action for all items receiving a negative response, in the central system file. A copy of the completed questionnaire and the associated plan for corrective action shall be forwarded to the "ISSO for USAID."

All questionnaire findings, supporting information and plans for corrective action may be used when M/IRM or SEC determines system certification, conducts system audits and inspections, and investigates security violations.

QUESTION	YES	NO
PERSONNEL SECURITY		
1. Do all personnel accessing the system have security clearances commensurate with the highest level of information authorized to be processed or stored on the system?		
2. Have all users signed an USAID classified System User Agreement?		
3. Have the facilities where classified information is processed or stored been designated restricted areas?		
TECHNICAL SECURITY		
1. Is classified national security information processed on either stand-alone TEMPEST microcomputers or local area networks specifically designed and authorized to accommodate such information?		
2. Is classified national security information printed on dedicated printers? (mission environments must employ laser printers.)		
3. Have all connections between microcomputers and printers used to process classified national security information and other automated information systems, networks, or communication devices been severed?		
4. Do microcomputers and printers that process classified national security information use power from the same electrical outlet or same multiple outlet strip?		
5. Is there a physical separation between TEMPEST-protected processing and printing equipment and other office equipment (lamps, fans, telephones, etc.), signal lines or metal conductors?		

QUESTION	YES	NO
6. Is there a 10-foot separation between transmitters (e.g., radios, base stations, transceivers, satellites, etc.) and all TEMPEST-protected equipment?		
7. Is there a 6-foot separation between equipment containing oscillators (non-TEMPEST data processing equipment, electronic office equipment, radios and televisions) and all TEMPEST-protected equipment?		
8. Is a spherical zone of control maintained around all equipment processing classified information? (RSO and/or "ISSO for USAID" have specifications for spherical zone of control.)		
ADMINISTRATIVE SECURITY		
1. Have U.S. citizens with TOP SECRET security clearances been formally appointed site ISSO and alternate?		
2. Have all personnel accessing the system been formally granted system access privileges via a memorandum from the Program Manager or Mission Director/Representative to the site ISSO?		
3. Are the screens of terminals used to process classified national security material facing away from windows and open access areas?		
4. Is system equipment use only to support official business?		
5. Is all system equipment labeled commensurate with the highest level of information authorized to be processed on the system?		
6. Have all storage media been labeled commensurate with the highest level of information authorized to be processed on the system?		
7. Are all removable storage media protected in accordance with the ADS Security. Chapter?		
8. Do only cleared U.S. citizen employees destroy classified media, output and equipment?		
9. Are floppy disks, magnetic tapes and classified output destroyed either by shredding or incineration?		
10. Have any security violations involving automated information system equipment been issued within the last 12 months?		
11. Were security violations involving automated information system equipment reported to the "ISSO for USAID" and SEC?		
12. Does the site ISSO randomly review all system storage media and equipment used within the mission or office to ensure National Security information is not being inappropriately processed or stored?		
13. Is a log maintained of all requested and/or performed maintenance service?		
14. Do all maintenance service personnel have security clearances commensurate with the highest level of information approved for processing or storage on the system?		
15. Have all system users received security awareness training?		
16. Have up-to-date system specific data, file, and record backup procedures been developed?		
17. Are system data, file, and record backup procedures regularly implemented?		
18. Are up-to-date contingency operation plans in place?		
19. Have the contingency operation plans been successfully practiced or implemented within the last 12 months?		
20. Have up-to-date disaster recovery and emergency action plans been developed?		

QUESTION	YES	NO
21. Have the disaster recovery or emergency action plans been successfully practiced or implemented within the last 12 months?		
22. Is a central system file maintained for each automated information system authorized to process classified national security information?		
23. Does the central system file contain the following documents (highlight the documents that are missing): risk assessment; classified user agreements and termination notices; contingency operation plans; disaster recovery plans; emergency action and destruction plans; applicable waivers or exceptions; approval to operate certificate; security reviews for the past two years; site ISSO and alternate appointments; system inventory; maintenance logs; visitors' logs; and, security container check sheets?		
24. Has the automated information system been formally approved to process classified national security information?		
PHYSICAL SECURITY		
1. Is the facility housing the automated information system authorized to store classified national security information?		
2. Is a routine security check made of all work areas housing systems authorized to process classified national security information?		
3. Do operating system and application software reside on removable hard drives?		
4. Are data, files and documents stored on removable storage media?		
5. Are removable storage media secured in approved security containers when not in use?		